

# Privacy Impact Assessments

## Core-Awareness-Training

The E-Government Act of 2002 (Public Law 107-347) mandates that federal agencies assess the impact to privacy from any new or substantially revised information collection, program, or Information Technology system. The document that results from this assessment is called a Privacy Impact Assessment (PIA).

Agencies are required to make PIAs publicly available, generally through the agency's official website.

## Adapted Privacy Impact Assessment for PM-ISE Social Media

### I. Overview and Purpose

The Office of the Program Manager for the Information Sharing Environment (PM-ISE) uses social media to support openness and transparency in government, enhance information sharing with ISE mission partners and stakeholders, and to solicit feedback and ideas about the information sharing environment from stakeholders and the public. PM-ISE utilizes three types of social media:

- Social networking sites, such as Facebook, LinkedIn, and GovLoop;
- Media sharing sites, such as YouTube and Flickr; and
- Blogs and online subscription services, such as Really Simple Syndication (RSS) feeds.

This adapted Privacy Impact Assessment (PIA)<sup>[1]</sup> analyzes the social media used by the PM-ISE, and addresses how public use of such tools may result in PM-ISE receiving or having access to personally identifying information (PII).

In addition, PM-ISE has developed the [PM-ISE Website Privacy Policy](#) <sup>[1]</sup> and the [PM-ISE Social Media and Comment Policy](#) <sup>[1]</sup> to inform public users of various social media policies and practices, as well as comment features on the official ISE.gov website.

### II. Data Management

#### **What personal information may become available to PM-ISE when individuals engage with PM-ISE on social media?**

Individuals need not provide any personal information in order to browse PM-ISE related content on social media. Any member of the public may visit the official ISE.gov website and blog or view official PM-ISE content hosted on third-party social media sites without establishing an account or providing any personal information.

Visitors who wish to participate actively in discussions by posting comments may need to provide certain personal information, depending on which of several avenues they choose for participating in the forum. Depending on the method selected, some PII would be available to PM-ISE.

Visitors who wish to comment on PM-ISE matters may do so directly through the official ISE.gov website and blog, or, alternatively, through third-party social media. The extent of personal information required in

each case follows.

### Official ISE.gov website

Individuals may interact (e.g., post a comment) directly through the official ISE.gov website in one of three ways:

- A. Post a comment as an "anonymous" user (no account);
- B. Login using an account specific to the official ISE.gov website; or
- C. Login through an Open Authorization<sup>[2]</sup> (OAuth) tool such as OpenID, Facebook Connect, or Sign in with Twitter.

**Anonymous user (Option A):** The user can submit comments to ISE.gov without creating a new account or logging in through an existing account. In this option, the word "anonymous" is displayed as the username. No PII is collected or made available to PM-ISE as part of this process.

**PM-ISE account (Option B):** The user must provide an e-mail address and generate a username and password. PM-ISE will store this limited account information on the ISE.gov website. However, PM-ISE system administrators will not have access to user-generated passwords. New usernames and passwords can be automatically generated by the system, at the request of the user. Users can also delete their accounts at any time. Once a user terminates his account, the account information will no longer be available to PM-ISE.

**Open Authorization (Option C):** The user must provide certain personal information to the selected third-party OAuth tool to establish an account. OAuth is a common open standard for authorization that allows users to engage with PM-ISE (or other site) from an existing account, without sharing the user's login credentials. Only limited information (a username and profile picture) will be made available to PM-ISE through the OAuth tool. No other PII is collected or made available to PM-ISE as part of this process.

In addition, PM-ISE officials and mission partners, officially interacting with the public on the ISE.gov website or on third-party social media, may populate their profiles with minimal PII, such as their name, photograph, and biographic information. This PII may be refreshed at any time by the subject and is not retained by PM-ISE.

### Third-Party Social Media

Individuals also may interact (e.g., post a comment) with PM-ISE from third-party sites.

In order to interact with PM-ISE on third-party social media sites, users must provide whatever personal information the owner of the third-party site requires to create an account. The PM-ISE does not receive any registration or account information from the individual site owner.

Depending on a user's security and privacy settings, some PII may be accessible by PM-ISE staff. However, PM-ISE will not collect, maintain, nor disseminate information about users who post comments, submit messages, or "follow," "friend," or "like" its official pages.

### **How will PM-ISE handle comments that include any PII made available by users?**

PM-ISE moderates<sup>[3]</sup> all comments submitted by users and will not post comments to the official ISE.gov website that do not adhere to its [PM-ISE Social Media and Comment Policy](#)<sup>[1]</sup> or that contain Social Security Numbers, home or business addresses, e-mail addresses, or phone numbers. PM-ISE will remove comments posted through third-party social media when content is inconsistent with the [PM-ISE Social Media and Comment Policy](#)<sup>[1]</sup> or contains sensitive PII. Each third-party social media site also will moderate comments consistent with its respective policy.

PM-ISE will not download comments; retrieve comments by a user's name or other personal identifier, or collect PII from comments posted to the official ISE.gov website or to official PM-ISE pages on third-party social media sites. No files will be maintained about individual users and their comments.

## III. Records Retention and Security

### How long will PM-ISE retain PII?

All comments and communications received from users through the use of social media, whether or not posted, will be retained according to federal law, and in compliance with the records management and disposition policies prescribed by the Office of the Director of National Intelligence, regardless of a user's action to terminate an account.

### How will PM-ISE secure PII?

PM-ISE will establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of all comments and communications retained, including controlled access limited to an authorized system administrator and the designated moderator for the performance of their official duties.

## IV. Privacy Act Requirements

### Will PM-ISE's activities on social media require the creation or modification of a system of records under the Privacy Act?

The PM-ISE's activities on the ISE.gov website and third-party social media will not trigger application of the Privacy Act<sup>[4]</sup> (i.e., the PM-ISE will not maintain or retrieve comments or account information by an individual's name or other unique identifier). Therefore, there is no requirement to establish a Privacy Act system of records.

## V. Privacy Risks and Mitigation

### What privacy risks are associated with PM-ISE's use of social media?

By its very nature, social media is designed to enable users to share personal information. Personal information is voluntarily provided by the user, and PM-ISE will not collect, maintain, or disseminate any PII. PM-ISE will use these tools in accordance with the [PM-ISE Website Privacy Policy](#)<sup>[1]</sup> and the [PM-ISE Social Media and Comment Policy](#)<sup>[1]</sup>. Therefore, the risk to a user's privacy resulting from engagement with the PM-ISE through social media is minimal.

- Risk: Depending on the privacy settings chosen by the user, some form of PII may be made available to PM-ISE staff or website administrators in the course of interacting with users on third-party social media and comment features.  
Mitigation: PM-ISE does not collect, maintain, or disseminate account or other information about individuals from third-party social media sites. Users who are concerned that personal information may be accessible to PM-ISE have the option of submitting comments on the official ISE.gov website as an "anonymous" user. Importantly, anyone can view the official ISE.gov website, blog, and official PM-ISE content on third-party social media sites without establishing an account.
- Risk: Users may inappropriately submit sensitive PII about themselves or others in comments, or include inappropriate hyperlinks (e.g., links to malicious software, fraudulent websites, etc.).  
Mitigation: PM-ISE will moderate comments containing sensitive PII or inappropriate content, whether the comments are submitted to the official ISE.gov website or blog, or through third-party

social media. With respect to comments submitted directly to ISE.gov, PM-ISE will moderate in accordance with the [PM-ISE Social Media and Comment Policy](#) <sup>[1]</sup>. Comments submitted to PM-ISE through third-party social media will be moderated by PM-ISE in accordance with that policy and also by the owner of the third-party site in accordance with its particular comment policy.

PM-ISE will provide notice on its official page at third-party sites that personal account information and PII contained in comments submitted to PM-ISE through third party sites is subject to the privacy and information handling policies of the third-party site owner.

## VI. Responsible Official

Kshemendra Paul,  
Program Manager, Information Sharing Environment  
Office of the Director of National Intelligence

## VII. Approving Official

Alexander W. Joel  
Civil Liberties Protection Officer  
Office of the Director of National Intelligence

---

<sup>1</sup>Office of Management and Budget Memorandum 10-23, ***Guidance for Agency Use of Third Party Websites and Applications*** (June 25, 2010), directs agencies to develop an adapted Privacy Impact Assessment (PIA) whenever an agency's use of a third party website or application makes personally identifiable information (PII) available to the agency.

<sup>2</sup>For more information on Open Authorization tools, [this OAuth Wikipedia article](#) <sup>[2]</sup> is helpful.

<sup>3</sup>For the purposes of this document, the term "moderate" means that PM-ISE will review all comments submitted to the official ISE.gov website, blog, and official PM-ISE third-party social media sites and reserves the right to not post, remove, or have removed comments that do not adhere to the Social Media and Comment Policy.

<sup>4</sup>See 5 U.S.C. § 552a, the Privacy Act of 1974.

---

**Source URL:** <http://www.ise.gov/privacy-impact-assessments>

### Links:

[1] <http://www.ise.gov/site-policies>

[2] <http://en.wikipedia.org/wiki/OAuth>